

# Technology Services Board

---

Security Subcommittee Meeting

May 9, 2024

9:00 am – 11:00 am

# Today's Agenda

9:00 am	Call to Order <ul style="list-style-type: none"><li>• Agenda Review</li><li>• Action: Approval of 2/8/24 Meeting Minutes</li><li>• New Members</li></ul>	Ralph Johnson
9:05 am	Action: TSB Security Subcommittee Charter - Review and Approval Recommendation	Ralph Johnson
9:15 am	OCS Highlight: Policy & Program Management ( <i>Discussion</i> )	Ralph Johnson
9:30 am	SLCGP Grant Update ( <i>Discussion</i> )	Zack Hudgins
9:40 am	Local and National Cybersecurity Coordination ( <i>Discussion</i> )	Ralph Johnson Bill Kehoe
10:00 am	Future Subcommittee Membership ( <i>Discussion</i> )	Ralph Johnson
10:10 am	Scheduling: Joint Meeting with Cybersecurity Advisory Committee of the Emergency Management Council (2SSB 5518 - 2023) ( <i>Discussion</i> )	Ralph Johnson Tristan Allen
10:20 am	Policy & Standard Review: <ul style="list-style-type: none"><li>• Action: Network Security Standard</li><li>• Action: Access Control Policy</li></ul>	Ralph Johnson
10:30 am	Executive Session: RCW 42.105.291(4)	Board Members
10:50 am	Public Comment	
10:55 am	Closing Remarks & Adjournment	Ralph Johnson

# TSB Security Subcommittee Charter: Review and Approval Recommendation

## **Purpose:**

To work together with a shared dedication to enhancing the security posture of Washington state as outlined in RCW 43.105.291. Address information security risks with urgency and regularly assess tools and services in the State of Washington ecosystem to achieve the objectives and safeguard the data and infrastructure of Washington state.

## **Objectives:**

As defined in RCW 43.105.291, the subcommittee will work to achieve .....

## Membership:

- State Chief Information Security Officer – Chair
- Technology Services Board Chair (State Chief Information Officer) – Co-Chair
- Chair of the Military Department’s Cybersecurity Advisory Committee
- (3) Technology Service Board Members
- (1) WaTech Executive Team Representative
- (1) Military Department Representative (in addition to the Chair of the Cybersecurity Advisory Committee)
- (2) Deputies from the Office of Cybersecurity
- (3) Local Government Representatives
- (3) Industry Representatives
- (2) Agency CIO/CISO Representatives
- (1) Representative from the Attorney General’s Office

## **Meetings:**

- Meetings will be held quarterly and scheduled for two hours unless otherwise designated.
- The subcommittee will hold at least one joint meeting annually with the Military Department's Cybersecurity Advisory Committee.
- Each meeting will discuss important security topics and events occurring in the state.
- Attendance at quarterly meetings will be in person and remote.

## **Charter Review:**

At least annually.

# OCS Highlight: Policy & Program Management

**Ralph Johnson**  
State Chief Information  
Security Officer (CISO)

Administrative  
Assistant

## SECURITY ENGINEERING

**Deputy CISO**  
**Matt Stevens**

Security Design Review  
Supervisor

Security Compliance  
Architecture Expert

Security Compliance  
Architecture Expert

Security Compliance  
Architecture Expert

Information Security  
Architect

Information Security  
Architect

## SECURITY OPERATIONS

**Deputy CISO**  
**Jack Potter**

Security Infrastructure Manager	Vulnerability Management Specialist
Information Security Platform Specialist	CIRT Analyst
Information Security Platform Specialist	CIRT Analyst
Information Security Platform Specialist	CIRT Analyst
Information Security Platform Specialist	Threat Hunter
Information Security Platform Specialist	Threat Hunter

## POLICY & PROGRAM MANAGEMENT

**Deputy CISO**  
**Kim Hort**

IT Security Specialist,  
Journey

IT Security Specialist,  
Journey

## INFORMATION SECURITY SERVICES

**Deputy CISO**  
**Tracy  
Auldredge**

Senior Information  
Security Supervisor, IT  
Security

IT Security Specialist,  
Journey

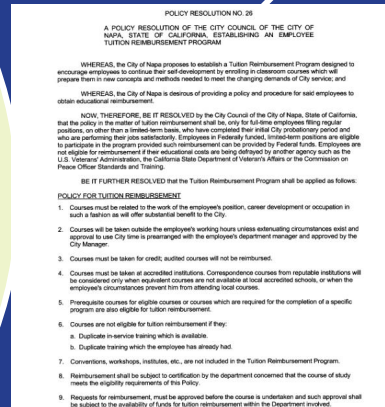
IT Security Specialist,  
Journey

IT Compliance Specialist



# Policy and Program Management

- Statewide Focus
- Information Security Policy and Standards Management and Maintenance
- Statewide Information Security Program Development
- Outreach



## Information Security Policy and Standards Management and Maintenance

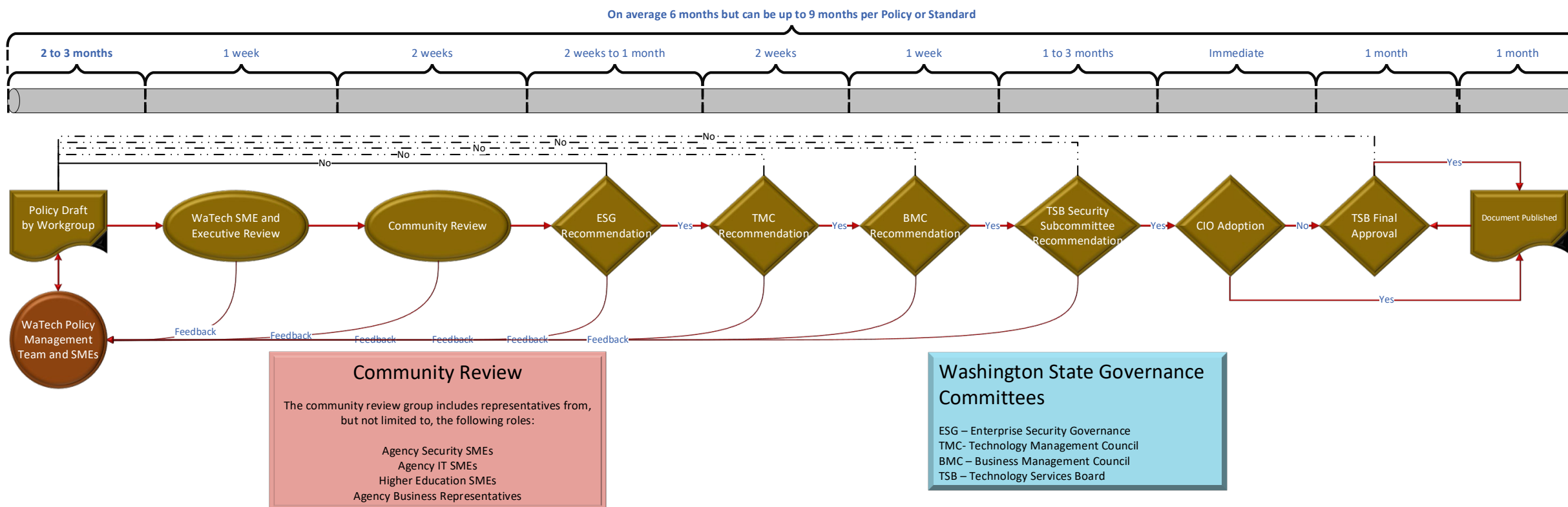


## OCIO Policy 141 & Standard 141.10 The Behemoth in the Beginning...

- 33-page security policy and standard document
- Not updated for over seven years.
- Content not vetted by the agency community.
- Not based on industry frameworks.
- No risk management integration.



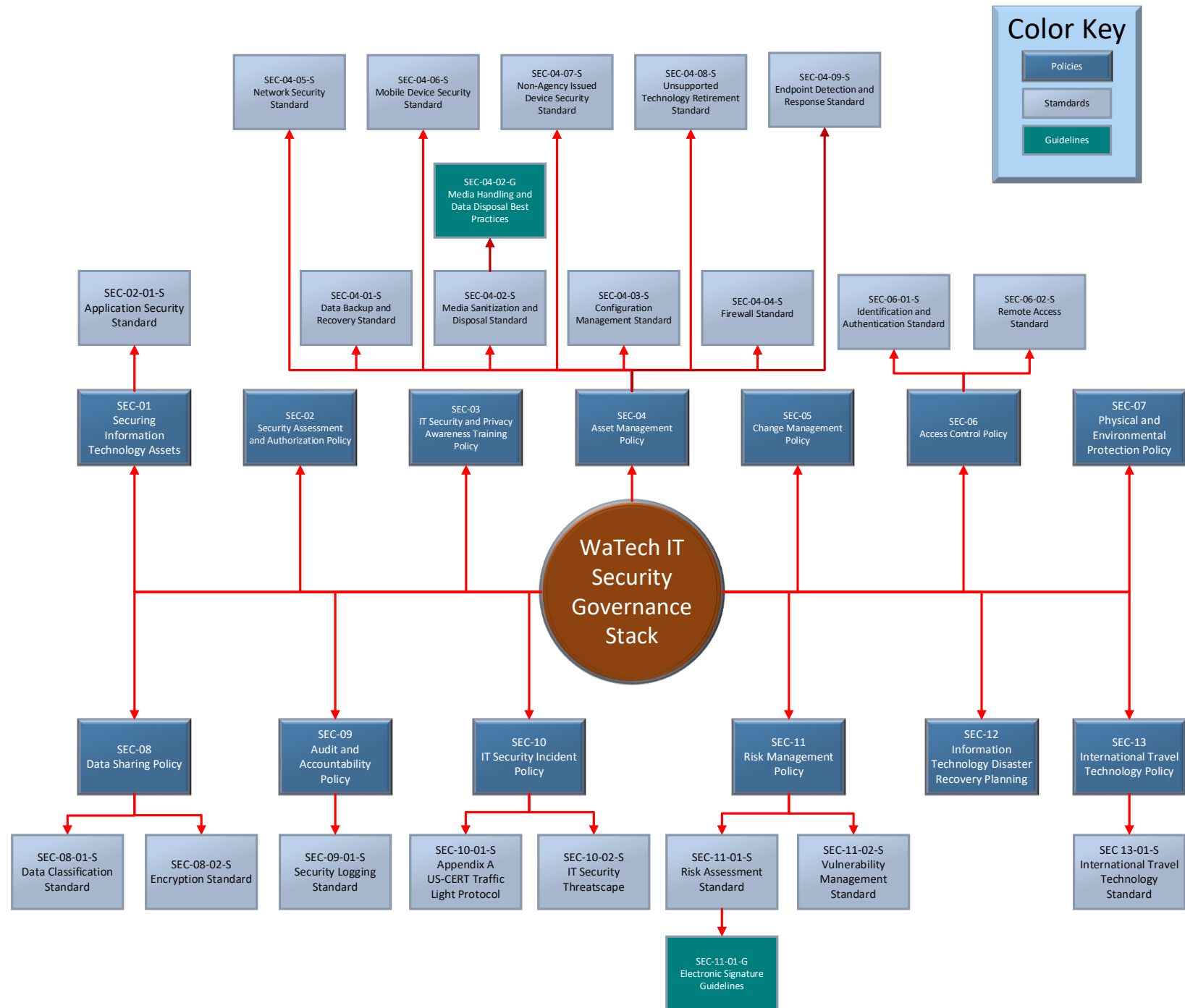
## WaTech IT Security Policy and Standards Development and Approval Process



# WaTech Policy Revision Crosswalk

Chapter 4: Security			Old #	New #	Name	Old #	New #	Name	Old #	New #		
Securing IT Assets	141, 141.10 1.1, 1.2, 1.3, 1.5, 1.6	SEC-01	Change Management Policy	141.10 8.1	SEC-05	Security IT Incident Policy ( <i>Pending</i> )					141.10 11	SEC-10
Securing IT Assets Standards	141.1	SEE BELOW				IT Security Incident Communication					143	Rescind
						Appendix-a - US- CERT Traffic Light Protocol					141.1	SEC-10-01-S
Security Assessment and Authorization Policy	141.10 1.2.1	SEC-02	Access Control Policy	141.10 6.1, 6.2	SEC-06	IT Security Threatscape					141.10b	SEC-10-02-S
Application Security Standard	141.10 7.1 - 7.4	SEC-02-01-S	Identification and Authentication Standard	141.10 6.3	SEC-06-01-S							
			Remote Access Standard	141.10 6.4	SEC-06-02	Risk Management Policy					141.10 1.2	SEC-11
Security Awareness & Training Policy	141.10 1.4	SEC-03				Risk Assessment Standard					141.10 1.3	SEC-11-01-S
			Physical and Environmental Protection Policy	141.10 2	SEC-07	Vulnerability Management Standard					141.10 5.5, 5.6	SEC-11-02-S
Asset Management Policy	141.10 8.2	SEC-04				Electronic Signature Guidelines					N/A	SEC-11-01-G
Data Backup and Recovery Standard	141.10 8.4	SEC-04-01-S	Data Sharing Policy	141.10 4.2	SEC-08-01-S	IT Disaster Recovery Planning					151	SEC-12
Media Sanitization and Disposal Standard	141.10 8.3	SEC-04-02-S	Data Classification Standard	141.10 4.1	SEC-08-01-S							
Media Handling and Data Disposal Best Practices	N/A	SEC-04-02-G	Encryption Standard	141.10 4.3, 4.4	SEC-08-02-S	International Travel Technology Policy					NEW	SEC-13
Configuration Management Standard	141.10 5.1.1	SEC-04-03-S				International Travel Technology Standard					NEW	SEC-13-01-S
Firewall Standard	141.10 5.1.2	SEC-04-04-S	Audit and Accountability Policy	141.10 1.6	SEC-09							
Network Security Standard	141.10 5.1-5.4	SEC-04-05-S	Security Logging Standard	141.10 10.1, 10.2	SEC-09-01-S							
Mobile Device Security Standard	141.10 5.8	SEC-04-06-S										
Non-Agency Issued Device Security Standard	N/A	SEC-04-07-S										
Unsupported Technology Retirement Standard	186	SEC-04-08-S										
Commonly Used Software Product Retirement	186.1	Strike										
Endpoint Detection and Response	141.10 5.7	SEC-04-09-S										

# IT Security Governance Stack



## Policy

### Definition of Terms Used in Policies and Reports

Search Policies

Chapter

- Please select -



Type

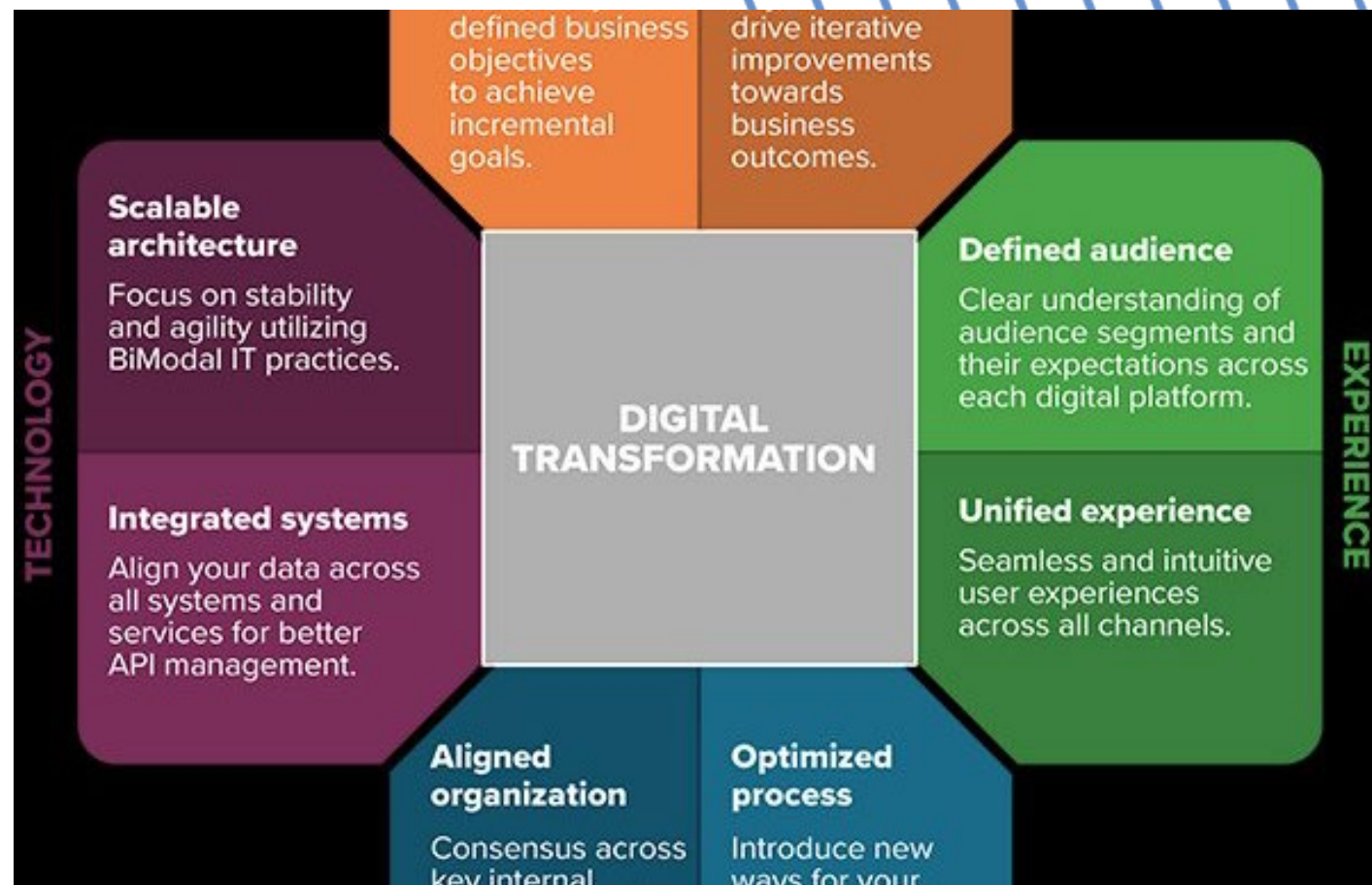
- Any -



Apply

Policy Title	Number	Chapter	Type
<a href="#">Technology Policies, Standards, and Procedures Policy</a>	POL-01 was 101	1. Policies on Policies	Policies
<a href="#">Naming Convention Standard</a>	POL-01-01-S was 101.1	1. Policies on Policies	Policies
<a href="#">Technology Policy &amp; Standard Waiver Request Standard</a>	POL-01-02-S was 103	1. Policies on Policies	Policies
<a href="#">Technology Policies and Standards Waiver Procedure</a>	POL-01-01-PR was 103.01	1. Policies on Policies	Procedures
<a href="#">Technology Portfolio Foundation</a>	MGMT-01 was 112	2. Management & Governance	Policies
<a href="#">Technology Portfolio Foundation - Applications</a>	MGMT-01-01-S was 112.10	2. Management & Governance	Standards
<a href="#">Technology Portfolio Foundation - Infrastructure</a>	MGMT-01-02-S was 112.20	2. Management & Governance	Standards
<a href="#">Managing Information Technology Portfolios Standards - Projects</a>	MGMT-01-03-S was 112.30	2. Management & Governance	Standards
<a href="#">Application Guidelines</a>	MGMT-01-0-1-G	2. Management & Governance	Guidelines

# Information Security Program Development



## Cybersecurity Training



# Why does Washington state need an Information Security Awareness Program?

Helps educate and empower employees by making them aware of cyber threats and what they can do to defend against them.  
It provides employees with the knowledge and skills to recognize and respond appropriately to security risks.



By providing layered tools and resources, such as videos, posters, assessments, and phishing simulations, organizations can build a culture of cybersecurity across their workforce.  
This helps reduce cyber risk by ensuring that employees understand their role in maintaining security.



Encourages a culture that promotes responsible handling of sensitive data, confidentiality, and adherence to security policies and procedures.  
When employees are aware of security best practices, they are more likely to follow them consistently.



Strong security requires a combination of technology, processes, and people. A security awareness program strengthens the people component of this strategy. It equips employees with the knowledge needed to protect sensitive information and prevent security incidents.

# Cybersecurity Awareness Video Modules

Video modules will raise awareness of cybersecurity threats relevant to the workforce, both in the workplace and their personal lives and that of their families.

- Information security basics
- Password and access management
- Protection from malicious code
- Phishing and other threats to email
- Social engineering
- Social media threats
- Proper data handling and the consequences of unintended exposures
- Recognizing and reporting incidents
- Uses of personal information technology
- Protection of information assets
- Information security and privacy policies

# Phishing Simulations

Phishing is a form of social engineering and scam where attackers deceive people into revealing sensitive information or installing malicious software.



 **phish**firewall

A person with long brown hair is seen from behind, sitting at a desk in a server room. They are looking at several computer monitors. The monitors display various data, including a world map, code, and system logs. The room is dimly lit, with the primary light source being the screens. The overall atmosphere is professional and technical.

**WaTech**

Washington Technology Solutions

# ***OCS UPDATE***

## **Security Alert Notices**

Identified threats were distributed by OCS in conjunction with other state agencies and trusted partners. The alerts are intended to raise users' awareness and aid them in protecting their data and personal data.

## **Hosted Learning Sessions**

The CISO, OCS personnel, and other information security professionals can deliver specialized training sessions.

“Lunch and Learn”

## **Special Events**

Cybersecurity Awareness Month  
Privacy Week

## **Compliance and Role Based Awareness**

## **Cybersecurity Awareness Library**

# Cyber Practitioner Training

---

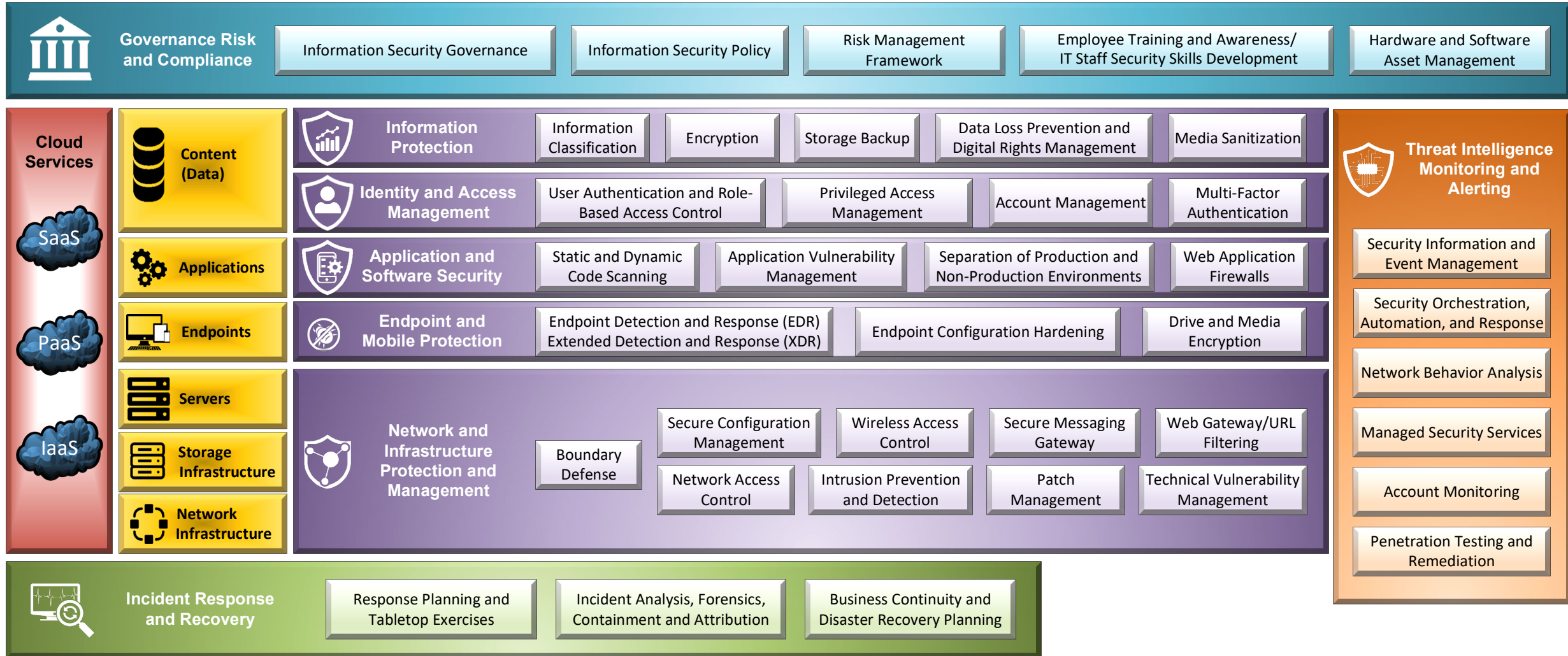


# WaTech

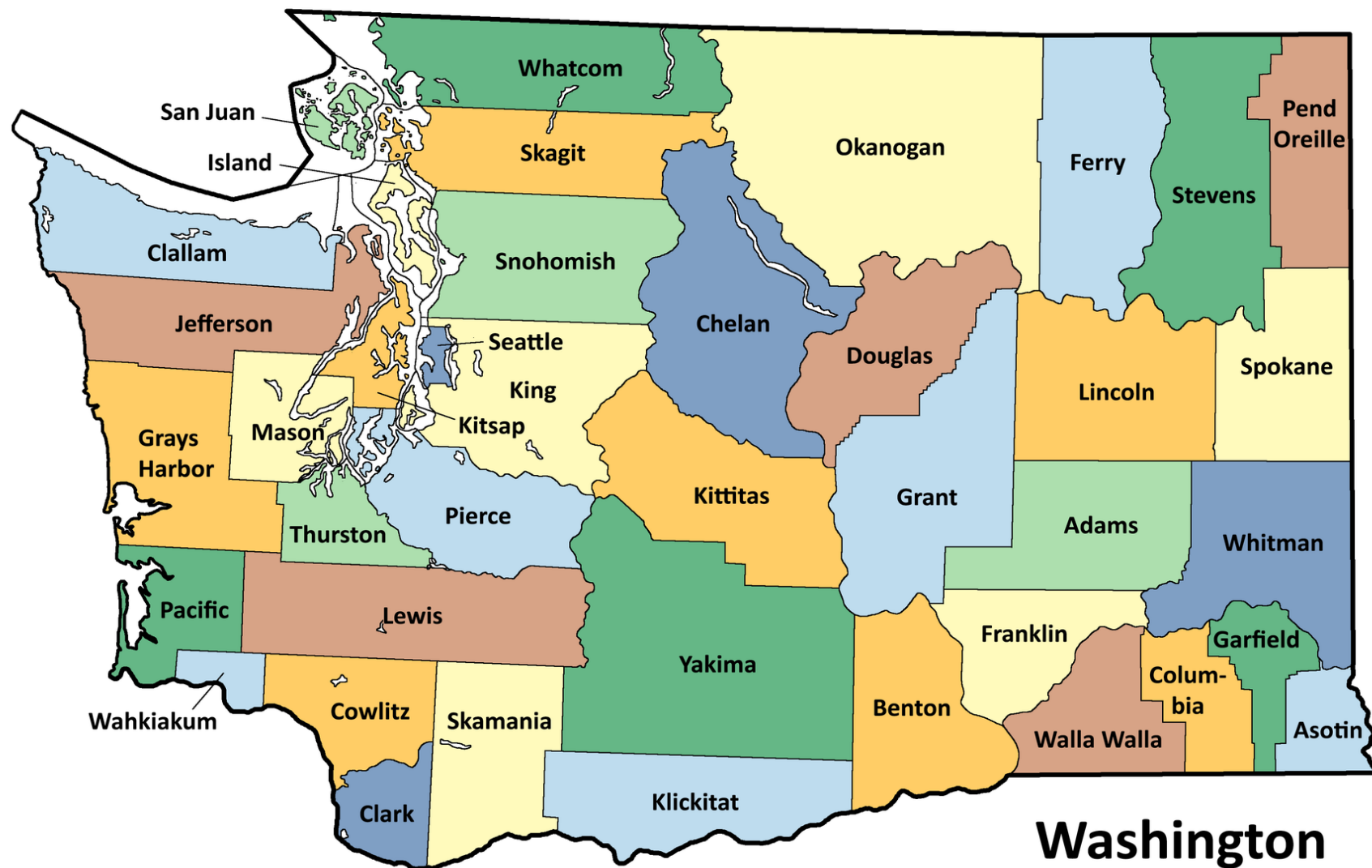
Washington Technology Solutions



## Strategic Information Security Architecture



# Outreach



## Outreach Efforts

- Participation with CISA, MS-ISAC and NASCIO
- Participation in ACCIS and other local associations
- Involvement in SAIC
- Presentations to local jurisdictions and groups
- Engagement with CISOs throughout the state
- SLCGP Grant

# State Local Cybersecurity Grant Program (SLCGP)

---

## SLCGP Overview

**Four-year federal government grant from Infrastructure Investment Jobs Act (IIJA).**

**Purpose:** Assist state, local, and tribal governments with managing and reducing systemic cyber risk, improving the security of critical infrastructure and the resilience of services.

**Eligibility:**

- Cities
- Counties
- Tribal partners
- Special Purpose Districts (including school districts)
- State agencies including higher education

*Match requirement provided by the State Legislature - Applicants will not need to provide matching funds*

## SLCGP Funding

- Four years of funding, Federal Fiscal Year (FY) 2022-2025
- Projected \$17.6 million – over 4 years
- Required match provided by the State Legislature for FY22 and 23 awards

	Fiscal Year	WA State Allocation	State 20%	Local 80%	Period of Performance
	FY22	\$3,666,530	\$733,306	\$2,933,224	12/1/2022-11/30/2026
	FY23	\$7,403,503	\$1,480,701	\$5,922,802	12/1/2023-11/30/2027
<b>PROJECTION</b>	FY24	\$5,308,000	\$1,061,600	\$4,246,400	12/1/2024-11/30/2028
	FY25	\$1,769,000	\$353,800	\$1,415,200	12/1/2025-11/30/2029
		<b>\$17,692,000</b>	\$3,629,407	\$14,517,626	

- 80% of the award must be obligated to local entities
  - 25% of the award must be obligated to rural entities (*population less than \$50K*)
- 20% of the award can be retained for state purposes/projects
  - 5% of the award for Management and Administration (M&A) of the award

## FY 23 – Current year

**Total funding remaining: \$5,337,861**

Portion of FY23 funding allocated during the FY22 solicitation round

- **Application solicitation timeframe:** March 29 – May 10, 2024
- **Results announced (*tentative*):** August 7-9, 2024
- **Funding available (*tentative*):** October 2024

## Allowable costs for the grant

- **Planning** - activities such as those associated with the development, review, and revision of the holistic, entity-wide cybersecurity plan and other planning activities that support the program goals and objectives
- **Organization** - program management, structures and mechanisms for information sharing between the public and private sector, and operational support
- **Equipment** - equipment used to address cybersecurity risks and cybersecurity threats to information systems owned or operated by, or on behalf of, state and local governments
- **Training** - establishment, support, conduct, and attendance of training and/or in conjunction with training by other federal agencies
- **Exercises** - expenditures related to exercise scenarios testing identified cybersecurity risks and threats
- **Management & Administration** - activities directly relating to the management and administration of SLCGP funds, such as financial management and monitoring (a maximum of up to 5% of the awarded funding)

## Grant requirements

### Each project must align with one Objective

**OBJECTIVE 1:** Develop and establish appropriate governance structures, as well as develop, implement, or revise **cybersecurity plans**, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.

**OBJECTIVE 2:** SLT agencies understand their current cybersecurity posture and areas for improvement based on continuous **testing, evaluation, and structured assessments**.

**OBJECTIVE 3:** Implement **security protections** commensurate with risk (outcomes of Objectives 1 & 2)

**OBJECTIVE 4:** Ensure organization personnel are appropriately **trained** in cybersecurity, commensurate with responsibility.

### Sign up for CISA services - required if funded:

- Cyber Hygiene Services (web application scanning and vulnerability scanning) [Free Cybersecurity Services and Tools: Cyber Hygiene Vulnerability Scanning | CISA](#)
- [Nationwide Cybersecurity Review \(NCSR\) \(cisecurity.org\)](#) - due by 12/31 each year

## Questions?

- **ALL applications submitted:** May 10, 2024
  - Email to [preparedness.grants@mil.wa.gov](mailto:preparedness.grants@mil.wa.gov)
- Technical assistance available:
  - Questions about allowable costs
  - Application issues
  - Grant requirements

### Contact:

***Grant and Application related questions:***  
**Melissa Berry, SLCGP Program Manager**  
[melissa.berry@mil.wa.gov](mailto:melissa.berry@mil.wa.gov)

***Project development and general Cybersecurity related questions***  
**Josh Castillo, Cyber Resilience Planner**  
[josh.castillo@mil.wa.gov](mailto:josh.castillo@mil.wa.gov)

***Planning Committee and Application scoring related questions***  
**Zack Hudgins, Privacy Manager**  
[zack.hudgins@watech.wa.gov](mailto:zack.hudgins@watech.wa.gov)

# Local and National Cybersecurity Coordination

# Cybersecurity Coordination

- Cybersecurity and Infrastructure Security Agency (CISA)
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Elections Infrastructure Sharing and Analysis Center (EI-ISAC)
- Federal Bureau of Investigations (FBI) and US Secret Service



**MS-ISAC®**

Multi-State Information  
Sharing & Analysis Center®



**Elections  
Infrastructure  
ISAC™**



## Cybersecurity Coordination

- Cybersecurity and Infrastructure Security Agency (CISA)
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Elections Infrastructure Sharing and Analysis Center (EI-ISAC)
- Federal Bureau of Investigations (FBI) and US Secret Service



**MS-ISAC**<sup>®</sup>  
Multi-State Information  
Sharing & Analysis Center<sup>®</sup>



**Elections  
Infrastructure  
ISAC**<sup>™</sup>





## CISA Services

- State and Local Cybersecurity Grant Program (SLCGP): CISA, in partnership with FEMA, provides grant funding to SLT governments through the SLCGP. This program addresses cybersecurity risks and threats to information systems owned or operated by SLT governments.
- Cybersecurity Advisors and Technical Experts: CISA has cybersecurity advisors and technical experts available year-round to work with SLT partners.
- Free Cybersecurity Services and Tools: CISA maintains a database of free cybersecurity services and tools for SLT governments and critical infrastructure organizations. These resources help reduce cybersecurity risk.
  - Cyber Hygiene Services: CISA's Cyber Hygiene services help secure internet-facing systems from weak configurations and known vulnerabilities.
  - Cybersecurity Performance Goal (CPG) Assessment: CISA's CPGs are a common set of practices that all organizations should implement to kickstart their cybersecurity efforts. Small- and medium-sized organizations can use the CPGs to prioritize essential actions with high-impact security outcomes.

## MS-ISAC and EI-ISAC Services

- MS-ISAC membership is open to all U.S. SLTT government organizations.
- EI-ISAC membership designed for all organizations involved in election processing
- Free services available to all members
  - Albert Sensor (Intrusion Detection System)
  - Malicious Domain Blocking and Reporting (MDBR)
  - Cyber Incident Response Team (CIRT)
  - Cybersecurity Advisory Services Program (CASP):
  - Cyber Threat Intelligence (CTI):



## FBI and US Secret Service

- Reporting of incidents
- Investigations of criminal activities



# Future Subcommittee Membership

# Current TSB Members

## Industry Members

Tanya Kumar – Oracle

## Legislative Members

Rep. Travis Couture – House R

Rep. Chipalo Street – House D

Sen. Matt Boehnke – Senate R

Sen. Joe Nguyen – Senate D

## Executive Branch (Agency Directors)

Bill Kehoe – State CIO & Chair

David Danner – UTC

Cami Feek - ESD

Tracy Guerin – DRS

## Other Government

Viggo Forde – Snohomish County

Andreas Bohman – UW-IT (Security Subcomm.)

**Activities:**

- Review emergent cyberattacks and threats to critical infrastructure sectors to identify gaps in state agency cybersecurity policies.
- Assess emerging risks to state agency information technology.
- Recommend a reporting and information-sharing system to notify state agencies of new risks, treatment opportunities, and projected shortfalls.
- Recommend tabletop cybersecurity exercises, including data breach simulation exercises.
- Assist the Office of Cybersecurity in developing best practice recommendations for state agencies.
- Review proposed policies and standards developed by the Office of Cybersecurity and recommend their approval to the full board.
- Review information relating to cybersecurity and ransomware incidents to determine commonalities and develop best practice recommendations for public agencies.
- Assist in developing the annual state of cybersecurity report.

## Proposed Membership Composition

- State Chief Information Security Officer – Chair
- State Chief Information Officer - Cochair
- Chair of the Military Department’s Cybersecurity Advisory Committee
- (3) Technology Service Board Members
- (1) WaTech Executive Team Representative
- (1) Military Department Representative
- (2) Deputies from the Office of Cybersecurity
- (3) Local Government Representatives
- (3) Industry Representatives
- (2) Agency CIO/CISO Representatives
- (1) Representative from the Attorney General’s Office
- Special Representative – WaTech’s ATG Counsel

- 18 identified members
- 13 confirmed
- 1 still unidentified

**Scheduling:  
Joint Meeting with  
Cybersecurity Advisory Committee of  
the Emergency Management Council  
(2SSB 5518-2023)**

**Purpose:** Provide advice and recommendations that strengthen cybersecurity in both industry and public sectors across all critical infrastructure sectors.

**Membership:** Organizations with expertise and responsibility for cybersecurity and incident response - local government, tribes, state agencies, institutions of higher education, the technology sector, and first responders.

**Activities:**

- Identify which local, Tribal, and industry infrastructure sectors are at the greatest risk of cyberattacks and need the most enhanced cybersecurity measures.
- Use federal guidance to analyze categories of critical infrastructure in the state that could reasonably result in catastrophic consequences if unauthorized cyber access to the infrastructure occurred.
- Recommend cyber incident response exercises related to risk and risk mitigation in the water, transportation, communications, health care, elections, agriculture, energy, and higher education sectors.
- Partners with the TSB Security Subcommittee.

## RCW 43.105.291 section 5 (2SSB 5518-2023)

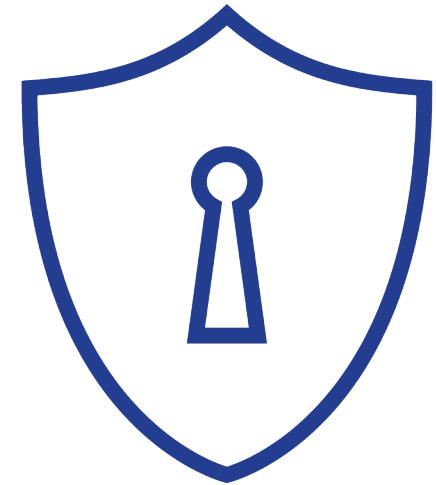
..... The technology services board security subcommittee must hold a joint meeting once a year with the cybersecurity advisory committee created in RCW 38.52.040 (*ESD cybersecurity advisory committee*).

**Joint Meeting Scheduled for  
September 26, 2024**

# Policy & Standard Review

## SEC-06 Access Control Policy

- Replaces 141.10 sections 6.1-6.2.
- Updates draw from NIST 800-53r5 and CIS Controls.
- Requires management of user accounts and roles.
- Requires exercising the Principle of Least Privilege.
- Minimizes impact of security breaches by limiting access.



## Network Security Standard

- Replaces Sections 5.1-5.4 of 141.10
- Establishes layered network security controls to ensure data...
  - Confidentiality
  - Integrity
  - Availability
- Aligns with industry standards



## VOTE

- Do you recommend that the TSB approve SEC-06 Access Control Policy and rescind 141.10 sections 6.1-6.2?
- Do you recommend approval of the Network Security standard and rescinding Sections 5.1-5.4 of 141.10?



# Executive Session:

**Executive Session in progress.**

**Resuming public meeting at**

# Public Comment



# Closing Remarks